APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/682,402	10/09/2003	Kyusun Chang	AUS920030685US1	8362

45371 7590 07/31/2007	EXAMINER
IBM CORPORATION (RUS)	LAFORGIA, CHRISTIAN A
c/o Rudolf O Siegesmund Gordon & Rees, LLp	

2100 Ross Avenue	ART UNIT	PAPER NUMBER
Suite 2600	2131	
DALLAS, TX 75201		

MAIL DATE	DELIVERY MODE
07/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/682,402	CHANG ET AL.
	Examiner	Art Unit
	Christian La Forgia	2131

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _23 April 2007_.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-6 and 8-31_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-6 and 8-31_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _09 October 2003_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1. The amendment of 23 April 2007 has been noted and made of record.

2. Claims 1-6 and 8-31 have been presented for examination.

3. Claims 7 and 32 have been cancelled as per Applicant's request.

Response to Arguments

4. Applicant's arguments with respect to claims 1-6 and 8-31 have been considered but are moot in view of the new grounds of rejection.

5. See further rejections that follow.

Claim Objections

6. Claim 5 is objected to because of recites "instructions for determining an appropriate rule to use to analyze the packet using the Virtual Local Area Network rules table table." For the purposes of examination, the Examiner shall construe the limitation to read, "instructions for determining an appropriate rule to use to analyze the packet using the Virtual Local Area Network rules table." Appropriate correction is required.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8.   Claims 1-6, 8-12, 16-19, 24-26, and 31 are rejected under 35 U.S.C. 102(a) and 35

U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication No. 2003/0041266 A1

to Ke et al., hereinafter Ke.

9.   As per claim 1, Ke teaches an apparatus comprising:

        a firewall having a processor and a memory (Figure 2 [block 210], paragraph 0033);

        wherein the firewall (Figure 2 [block 210], paragraph 0033, 0034, i.e. firewall does some

routing, such as determine the intended VLAN for the packet and attaching an appropriate

VLAN tag) is part of a router (Figure 2 [block 205], paragraph 0033) that creates a plurality of

Virtual Local Area Networks (Figure 2 [blocks 230, VLAN1, VLAN2, VLAN3, VLAN4]) using

a network switch (Figure 2 [block 225], paragraph 0033);

        wherein the network switch is connected to the firewall (Figure 2 [block 225], paragraph

0033);

        wherein the memory contains a Virtual Local Area Network rules table (paragraphs 0053,

0055, i.e. policy-based and session-based lookup table, classification policies);

        wherein the Virtual Local Area Network rules table allows an administrator to designate

a trust level for each of the plurality of Virtual Local Area Networks (paragraphs 0039, 0059-

0122, i.e. a user interface that allows a user to set incoming and outgoing policies for the

VLANS and authentication policies);

        wherein only the firewall is used to protect each of the plurality of Virtual Local Area

Networks in accordance with a designated trust level (paragraph 0033, i.e. the firewall **210** acts

as a common firewall for all the customers).

10.   Regarding claims 2, 16, 19, 23, 26, and 30, Ke teaches a table defining the relationship

between the trust levels, the rules, and the plurality of Virtual Local Area Networks (paragraphs

0053, 0055, i.e. policy-based and session-based lookup table, classification policies).

11.   With regards to claims 3 and 11, Ke teaches wherein the firewall comprises a

configuration program, wherein the configuration program allows a user to add, delete, or

modify the Virtual Local Area Network rules table and a plurality of trust levels in the Virtual

Local Area Network rules table (paragraphs 0039, 0059-0122 i.e. a user interface that allows a

user to set incoming and outgoing policies for the VLANS and authentication policies).

12.   With regards to claims 4 and 12, Ke teaches wherein the firewall further comprises: a

security program, wherein the security program analyzes a packet and determines if the Virtual

Local Area Network rules table permits or denies the packet (paragraphs 0046-0058).

13.   Concerning claims 5, 14, 21, and 28, Ke teaches wherein the security program comprises:

        instructions for determining a destination of the packet (paragraphs 0048, 0050,

extracting layer 2 and 3 information, including TCP/UDP port information);

        instructions for determining an appropriate rule to use to analyze the packet using the

Virtual Local Area Network rules table (Figure 5 [block 515], paragraphs 0049-0050);

        instructions for analyzing the packet using the appropriate rule (Figure 5 [block 520] ,

paragraphs 0049-0050);

instructions for determining if the packet is permitted under the appropriate rule (Figure 5

[block 525], paragraph 0051);

responsive to a determination that the appropriate rule permits the packet, instructions for

permitting the packet (Figure 5 [blocks 535, 540], paragraph 0051); and

responsive to a determination that the rules deny the packet, instructions for denying the

packet (Figure 5 [block 530], paragraph 0051).

14.   Concerning claims 6, 15, 18, 22, 25, and 29, Ke teaches responsive to a determination

that the rules do not permit or deny the packet, instructions for denying the packet (Figure 5

[block 530], paragraph 0051).

15.   As per claim 8, Ke teaches a router (Figure 2 [block 205], paragraph 0033) comprising:

a switch (Figure 2 [block 225], paragraph 0033) connected to a firewall (Figure 2 [block

210], paragraph 0033, 0034, i.e. firewall does some routing, such as determine the intended

VLAN for the packet and attaching an appropriate VLAN tag) and a plurality of computer

networks (Figure 2 [blocks 230, VLAN1, VLAN2, VLAN3, VLAN4]); and

wherein the firewall allows an administrator to configure a plurality of trust levels and

associate a trust level with each of the plurality of computer networks (paragraphs 0039, 0059-

0122, i.e. a user interface that allows a user to set incoming and outgoing policies for the

VLANS and authentication policies);

wherein the firewall serves each of the plurality of computer networks in accordance with the trust level associated with each of the plurality of computer networks (paragraphs 0046-0058).

16.   Regarding claim 9, Ke teaches wherein the switch comprises a sub-switch: the sub-switch being assigned one of a plurality of trust levels (Figure 2 [blocks 235], paragraph 0033).

17.   Regarding claim 10, Ke teaches wherein the firewall analyzes a packet using some of the rules (paragraphs 0046-0058); and

wherein the rules used in the lower trust levels are excluded from the rules used to analyze the packet (paragraphs 0046-0058).

18.   As per claims 17 and 24, Ke teaches a method and program product for analyzing a packet using a firewall which, creates a plurality of trust levels for a plurality of computer networks, the method comprising:

using a single router containing firewall to service each of the plurality of computer networks (Figure 2 [block 210], paragraph 0033, 0034, i.e. firewall does some routing, such as determine the intended VLAN for the packet and attaching an appropriate VLAN tag) by performing the steps of:

determining the destination of the packet (paragraphs 0048, 0050, extracting layer 2 and 3 information, including TCP/UDP port information);

accessing a plurality of rules (Figure 5 [block 515], paragraphs 0049-0050);

determining an appropriate rule to use to analyze the packet (Figure 5 [block 515],

paragraphs 0049-0050);

analyzing the packet using the rules (Figure 5 [block 520] , paragraphs 0049-0050);

determining if the packet is permitted under the rules (Figure 5 [block 525], paragraph

0051);

responsive to a determination that the rules permit the packet, permitting the packet

(Figure 5 [blocks 535, 540], paragraph 0051);

and

responsive to a determination that the rules deny the packet, denying the packet (Figure 5

[block 530], paragraph 0051).

19.   As per claim 31, Ke teaches a firewall capable of creating a plurality of trust levels for a

plurality of computer networks comprising:

a router (Figure 2 [block 205], paragraph 0033) containing the firewall (Figure 2 [block

210], paragraphs 0033, 0034, i.e. firewall does some routing, such as determine the intended

VLAN for the packet and attaching an appropriate VLAN tag);

a plurality of rules (Figures 5 [blocks 515, 520], paragraphs 0049-0050, i.e. traffic

policies and classification rules);

a table defining the relationship between the trust levels, the rules, and the computer

networks (paragraphs 0053, 0055, i.e. policy-based and session-based lookup table, classification

policies);

a configuration program, wherein the configuration program allows a user to add, delete, or modify the rules and trust levels in the table (paragraphs 0039, 0059-0122 i.e. a user interface that allows a user to set incoming and outgoing policies for the VLANS and authentication policies);

a security program, wherein the security program analyzes a packet and determines if the rules permit or deny the packet (paragraphs 0046-0058), the security program comprising:

instructions for determining the destination of the packet (paragraphs 0048, 0050, extracting layer 2 and 3 information, including TCP/UDP port information);

instructions for determining the appropriate rules to use to analyze the packet using the table (Figure 5 [block 515] , paragraphs 0049-0050);

instructions for analyzing the packet using the rules (Figure 5 [block 520] , paragraphs 0049-0050);

instructions for determining if the packet is permitted under the rules (Figure 5 [block 525], paragraph 0051);

responsive to a determination that the rules permit the packet, instructions for permitting the packet (Figure 5 [blocks 535, 540], paragraph 0051);

responsive to a determination that the rules deny the packet, instructions for denying the packet (Figure 5 [block 530], paragraph 0051); and

responsive to a determination that the rules do not permit or deny the packet, instructions for denying the packet (Figure 5 [block 530], paragraph 0051),

wherein only the firewall is used to protect each of the plurality of computer networks (paragraph 0033, i.e. the firewall **210** acts as a common firewall for all the customers).

Claim Rejections - 35 USC § 103

20.   The text of those sections of Title 35, U.S. Code not included in this action can be found

in a prior Office action.

21.   Claims 13-15, 20-23, and 27-30 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Ke.

22.   With regards to claim 13, Ke teaches wherein the security program comprises:

        instructions for determining the sub-switch location of the packet (paragraphs 0033-

0034);

        instructions for determining a source of the packet (paragraphs 0047, 0052, i.e.

determining if the incoming packet is from a trusted or untrusted interface);

        instructions for determining a destination of the packet (paragraphs 0048, 0050,

extracting layer 2 and 3 information, including TCP/UDP port information).

23.   Ke does not teach determining if the packet is attempting to go to a higher trust level; and

responsive to a determination that the packet is not attempting to go to a higher trust level,

permitting the packet.

24.   It would have been obvious to one of ordinary skill in the art at the time the invention

was made to determine whether the packet was attempting to go to a higher trust level, and if it

was determined that the packet was not attempting to go to a higher trust level, permitting the

packet, since Ke discloses at paragraphs 0039, 0059-0122 a system for configuring the rules and

policies of the firewall system. Since Ke discloses a system for establishing rules and policies,

the Applicant's determination step would only require routine skill in the art to program into the

firewall policy engine.

25.   As per claims 20 and 27, Ke teaches a method and program product for analyzing a

packet using a firewall which creates a plurality of trust levels for a plurality of computer

networks, the method comprising:

using a single router containing the firewall to service each of the plurality of

computer networks (Figure 2 [block 210], paragraph 0033, 0034, i.e. firewall does some routing,

such as determine the intended VLAN for the packet and attaching an appropriate VLAN tag) by

performing the steps of:

determining the sub-switch location of a packet (paragraphs 0033-0034);

determining a source of the packet (paragraphs 0047, 0052, i.e. determining if the

incoming packet is from a trusted or untrusted interface);

determining a destination of the packet (paragraphs 0048, 0050, extracting layer 2 and 3

information, including TCP/UDP port information).

26.   Ke does not teach determining if the packet is attempting to go to a higher trust level; and

responsive to a determination that the packet is not attempting to go to a higher trust level,

permitting the packet.

27.   It would have been obvious to one of ordinary skill in the art at the time the invention

was made to determine whether the packet was attempting to go to a higher trust level, and if it

was determined that the packet was not attempting to go to a higher trust level, permitting the

packet, since Ke discloses at paragraphs 0039, 0059-0122 a system for configuring the rules and

policies of the firewall system. Since Ke discloses a system for establishing rules and policies,

the Applicant's determination step would only require routine skill in the art to program into the firewall policy engine.

Conclusion

28.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

29.   The following patents are cited to further show the state of the art with respect to managing VLANs via a firewall, such as:

United States Patent No. 7,093,280 B2 to Ke et al., which is cited to show the patent that issued from the prior art that was applied.

United States Patent Application Publication No. 2006/020986 A1 to Ke et al., which is cited to show a co-pending application that is related to the applied prior art.

United States Patent Application Publication No. 2002/0073337 A1 to Ioele et al., which is cited to show a router containing a firewall in paragraph 0035.

30.   Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

31.   A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

32.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

33.   If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

34.   Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

CHRISTOPHER REVAK
PRIMARY EXAMINER